Templating the Information Threat

By David C. Grohoski, Lieutenant Colonel , U.S. Army
and Marc J. Romanych, Major, U.S. Army (Retired)

Editorial Abstract: *Successful information operations are dependent on detailed and often specialized intelligence support. In this article Colonel Grohoski and Major Romanych share techniques developed at the Land Information Warfare Activity (LIWA) for templating an adversary's information capabilities and vulnerabilities. The techniques suggested in this article constitute one approach to conducting an information intelligence preparation of the battlespace.*

According to Joint and US Army doctrine, successful information operations (IO) are dependent on a detailed and thorough intelligence preparation of the battlespace (IPB). However, doctrine, to include Joint Publications 3-13, *Joint Doctrine for Information Operations*, and 2-01.3, *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*, as well as Service publications such as Army Field Manuals 100-6, *Information Operations*, and 34-130, *Intelligence Preparation of the Battlefield*, does not explain how to conduct an information IPB.[1] Thus, IO staffs are left unaided when developing techniques for analyzing the information environment.

Experience gained by personnel from the US Army Land Information Warfare Activity (LIWA) demonstrates that analyzing the information environment is relatively straightforward. By applying the methodology used to describe the conventional battlespace environment to an analysis of the information environment, planners can define the information environment and describe its characteristics. However, IO staffs lack the doctrinal procedures to determine an adversary's ability to conduct operations in the information environment. This article offers techniques for templating an adversary's information capabilities and vulnerabilities as a means to evaluate the threat.[2] Our intent is to stimulate dialogue on other information IPB techniques and procedures.

Why is Modeling Necessary?

To understand how an adversary operates in the information environment, IPB analyzes the adversary's information system and how that system collects, processes, disseminates, and uses information.[3] Modeling, a combination of graphic depictions (i.e., templates) and written descriptions, is one method. By developing templates describing doctrine and tactics, analysts can gain an understanding of the adversary's capabilities, vulnerabilities, and susceptibilities in the information environment and how that adversary will operate in the information environment to support a potential course of action (COA).

Before describing some templating techniques, consider that if an information IPB and its products are to be valid, then the analysis must be conducted as part of, or at least built upon, the IPB of the conventional battlespace. Information IPB is not a separate analytical process. If conducted in isolation, information IPB and its products will likely fail to adequately describe the information environment accurately, and reliably predict adversary actions in that environment.

Templating the Adversary's Information System

During step three of IPB (Evaluate the Adversary), analysts can evaluate the adversary's information system by identifying those assets and functions (e.g., decision makers, information infrastructure, and decision making processes) the adversary requires to operate effectively. This process also helps determine how the adversary will attack our information systems and defend its own. While there are many ways to model an information system, three useful templates include: the decision-making, information infrastructure, and information tactics templates.[4] In sum, these templates portray the doctrinal composition and organization of the adversary's information system with emphasis on command and control and offensive and defensive information capabilities. The result identifies adversary information system strengths, vulnerabilities, and susceptibilities; and serves as the IO section's input to the intelligence staff's overall IPB. The products described in this article are not stand-alone products, but are meant to feed the overall IPB process.

Decision-Making Template. The decision-making template describes "who" in an organization makes decisions. It profiles an adversary organization by depicting the structure and general characteristics of the organization and identifies key decision makers, describing their personal attributes. The purpose of the templating is to determine how an organization operates to achieve its mission or goals. It depicts the decision-making process of both individual adversary leaders and the adversary organization as a whole.

Construction of the template begins with charting the organization's formal and informal structures. Then, critical linkages and associated relationships of the organization are determined and key decision makers are identified. Pairing key leaders' positions to the decision-making characteristics of the organization leads to an analysis of how the organization plans, supervises, and coordinates the activities of its subordinate elements. It is then possible to surmise how the organization interacts to make decisions. Figure 1 demonstrates a method for developing a decision-making template.

When building the decision-making template the following aspects may be considered:

- Structure of the organization. All organizations, whether military or civilian, are created to accomplish a specific purpose or goal. The formal structure of an organization is only an outline. To determine (or deduce) internal processes, the informal structure may be the key. In some organizations (e.g., insurgent or para-military), there may only be an informal structure. Always look for special staffs and sub-elements of the organization that may have a direct relationship to the operation of the organization. These elements are likely to be important.

- Critical linkages and interrelationships. Identifying key leaders is more than just selecting an organization's senior personnel. Formal positions of authority do not always equate to power and influence in the organization. The informal side of the organization must be analyzed as well. Key leaders may be those individuals who are prominent on both the formal and informal sides of the organization. It is also important to determine what outside individuals or elements have a relationship with the organization under analysis. A detailed analysis will consider all possible linkages (e.g., military to health, religious, education, industrial organizations, etc.). At this point it is not necessary to contemplate why a relationship occurs, only to note its existence. Once links and relationships are identified, the last step is to determine who in the organization makes the decisions.

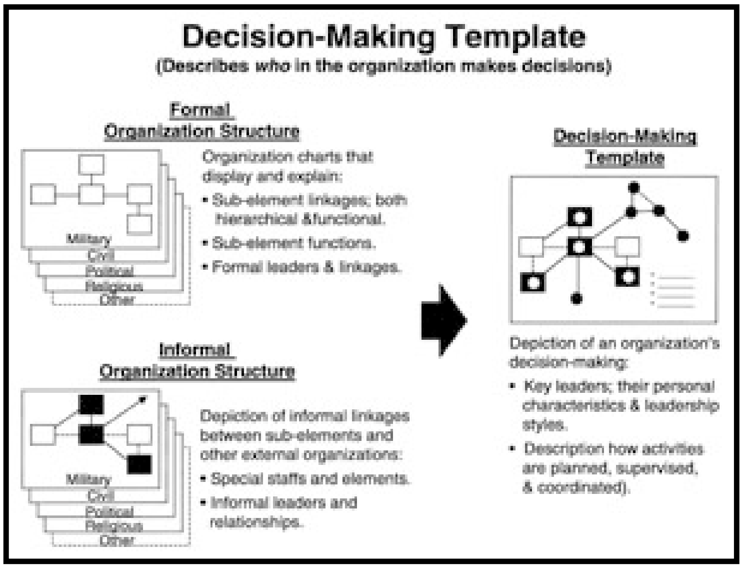
Decision-Making Template
(Describes who in the organization makes decisions)
Formal Organization Structure
Military
Civil
Political
Religious
Other
Organization charts that display and explain:
• Sub-element linkages; both hierarchical &functional.
• Sub-element functions.
• Formal leaders & linkages.
Informal Organization Structure
Military
Civil
Political
Religious
Other
Depiction of informal linkages between sub-elements and other external organizations:
• Special staffs and elements.
• Informal leaders and relationships.
Decision-Making Template
Depiction of an organization's decision-making:
• Key leaders; their personal characteristics & leadership styles.
• Description how activities are planned, supervised, & coordinated).

Figure 1. Constructing a Decision-Making Template

- Key decision makers. Once identified, key decision makers should be characterized as to their personality types and leadership styles (e.g., democratic or authoritative). The aggregate leadership style of the senior leaders is likely to be indicative of the entire organization's decision-making.

- Decision-making characteristics. It may not be possible to actually identify the decision-making processes of an organization. However, determining a few key characteristics such as the cohesiveness of the organization's members, the size and number of subordinate elements, or the collective attributes of the leaders, may provide insight as to how the organization makes decisions (e.g., centralized versus decentralized) and how it will behave as a collective entity.

Information Infrastructure Template. The information infrastructure template depicts "what" nodes, links, assets, and means an organization uses to collect, process, and disseminate information. Building the template is challenging but straightforward. First, a graphic display of the nodes, links, and systems is developed. Included in the graphic are the relevant technical aspects (e.g., equipment types and operating parameters, etc.) for each information system. This information is then applied against the structure of the organization as depicted by the decision-making template to provide a template of what equipment and means support the key decision makers. When completed, the template provides an understanding of the information infrastructure's critical systems and linkages. Figure 2 demonstrates a method for developing an information infrastructure template.

When building the information infrastructure template the following aspects may be considered:

- Information nodes and links. Traditional links and nodes are command posts, signal sites (AM, FM, UHF, VHF, satellite, etc.), electronic collection/sensor sites, and telephone switches. When analyzing non-military organizations, nodes may be meeting places such as offices and civic centers or even gathering places such as a park or a cafe. In these cases, human interface (face-to face meetings or couriers) rather than technology may be the critical link between nodes.

- Communications means. Communication means are more than just telephone, internet, and radio systems. Mass communications such as print and broadcast media may also provide important means.

- Supporting systems. Components that provide critical support to an information system, such as electrical power, may be more accessible and vulnerable to IO effects than the information system itself.

Information Tactics Template. A tactics model describes "how" the adversary will employ all available information assets. This includes identifying and assessing those assets the adversary can use, how each asset is doctrinally employed to attack and protect information systems, and where the assets will be doctrinally employed based on operating parameters. The sum of this analysis determines what the adversary force can do (i.e., its capabilities) to exploit or deny our information and information systems (offensive activities) while safeguarding its own information and information systems (defensive activities). An information tactics template attempts to describe how the adversary will: shape the information environment, mange information, and control the range of available options. It is important that the template is constructed in concert with the corresponding tactics models developed by the intelligence staff. Figure 3 describes how to build an information tactics template.

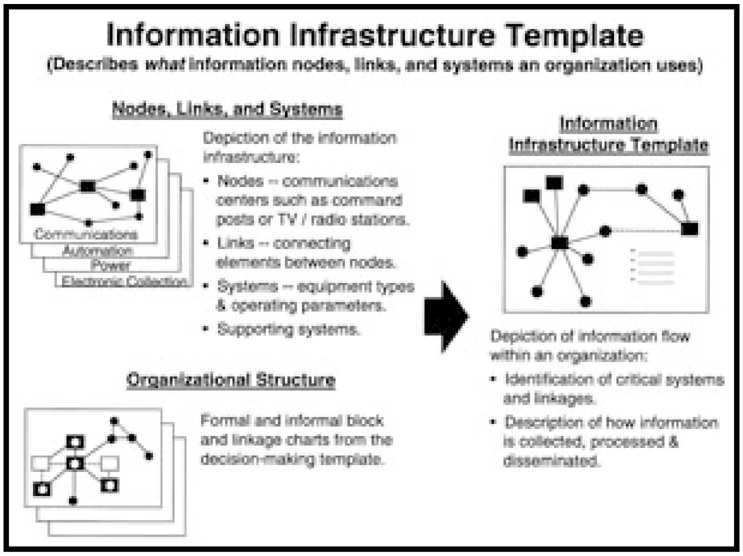
Information Infrastructure Template
(Describes *what* information nodes, links, and systems an organization uses)
Nodes, Links, and Systems
Communications
Automation
Power
Electronic Collection
Depiction of the information infrastructure:
• Nodes -- communications centers such as command posts or TV / radio stations.
• Links -- connecting elements between nodes.
• Systems -- equipment types & operating parameters.
• Supporting systems.
Organizational Structure
Formal and informal block and linkage charts from the decision-making template.
Information Infrastructure Template
Depiction of information flow within an organization:
• Identification of critical systems and linkages.
• Description of how information is collected, processed & disseminated.

Figure 2. Constructing an Information Infrastructure Template

The following specific aspects may be considered when building an information tactics template:

- Doctrine. In lieu of definitive information concerning doctrine and past operations, the template addresses possible (and feasible) options the adversary has when employing its assets. Much of this is predicated on knowing the assets available and their associated operating parameters. Caution must be exercised to not portray adversary actions as a mirror image of our own doctrine and perceptions. Adversary concepts and processes for attacking and defending information and information systems will not equate to our own.

- Information assets. Consider any assets that can be used to influence the information environment (e.g., collection and monitoring equipment, HUMINT resources, access to satellites, public information, propaganda, jamming systems, early warning systems, etc.).

- Employment of information assets. Determine how each information asset contributes to the operation as well as any offensive or defensive application.

Templating Adversary Information Activities

As part of determining adversary COAs (step four of IPB), information IPB postulates how, when, where, and why (to what purpose) the adversary will use its information systems to support its likely objectives and achieve its desired end state. To be valid, this analysis must be developed in concert with, and integrated into, the intelligence staff's situation templates. Ideally, the adversary's information activities are depicted on the G2/S2 situation template. If necessary, a separate or supporting information situation template can be constructed to provide clarity.

An information situation template depicts how the adversary will employ its information systems to achieve information superiority. To develop the template, critical information assets, capabilities, and vulnerabilities (taken from templates developed in the previous step of IPB) are analyzed relative to the effects of the battlespace and information environment, and importantly, as compared to the adversary's anticipated scheme of maneuver. This analysis provides an overall concept and supporting objectives for the adversary's information activities by applying the adversary's information capabilities and vulnerabilities to the scheme of maneuver. Next, the probable location of information assets are identified and each asset's role in the operation is defined by assigning a possible task and purpose. The final step is to identify those assets (i.e., individuals, organizations, nodes, links, and systems) critical to the adversary commander's ability to operate in the information environment. These assets, when weighed against the adversary's overall course of action, may become high-value

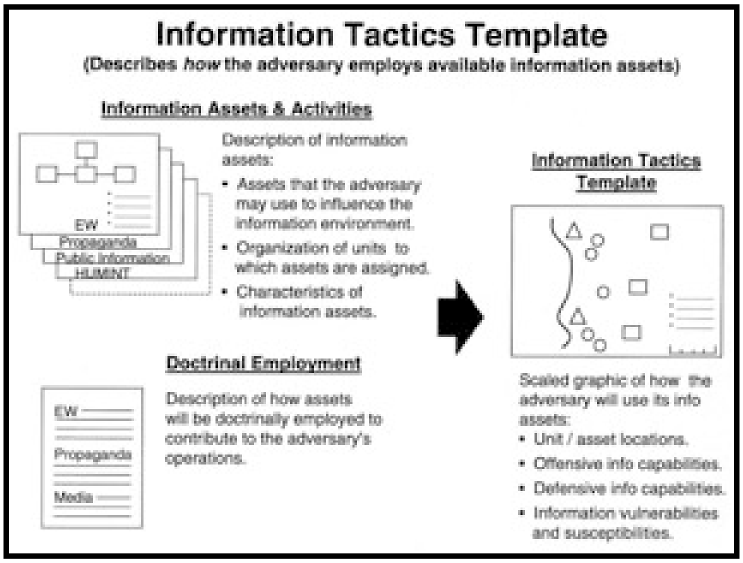
Information Tactics Template
(Describes *how* the adversary employs available information assets)
Information Assets & Activities
EW
Propaganda
Public Information
HUMINT
Description of information assets:
• Assets that the adversary may use to influence the information environment.
• Organization of units to which assets are assigned.
• Characteristics of information assets.
Doctrinal Employment
EW
Propaganda
Media
Description of how assets will be doctrinally employed to contribute to the adversary's operations.
Information Tactics Template
Scaled graphic of how the adversary will use its info assets:
• Unit / asset locations.
• Offensive info capabilities.
• Defensive info capabilities.
• Information vulnerabilities and susceptibilities.

Figure 3. Constructing a Information Tactics Template

targets. Figure 4 demonstrates a method for constructing an information situation template.

An important element of a situation template is time. The template must predict when in the operation the adversary will employ its information system and assets. Thus, for example, by anticipating when and where the adversary may jam friendly radio nets, the friendly commander can initiate appropriate counter-measures. This is possible by using the time and phase lines associated with the scheme of maneuver. It is also important to determine the adversary commander's decision points and probable decisions at those decision points. These are used when planning of the friendly scheme of maneuver to determine when and where in the battlespace the friendly forces must focus IO to achieve information superiority. It may be useful to develop the information situation template to show how the adversary's information system and assets will be employed at the time of its critical decision points.

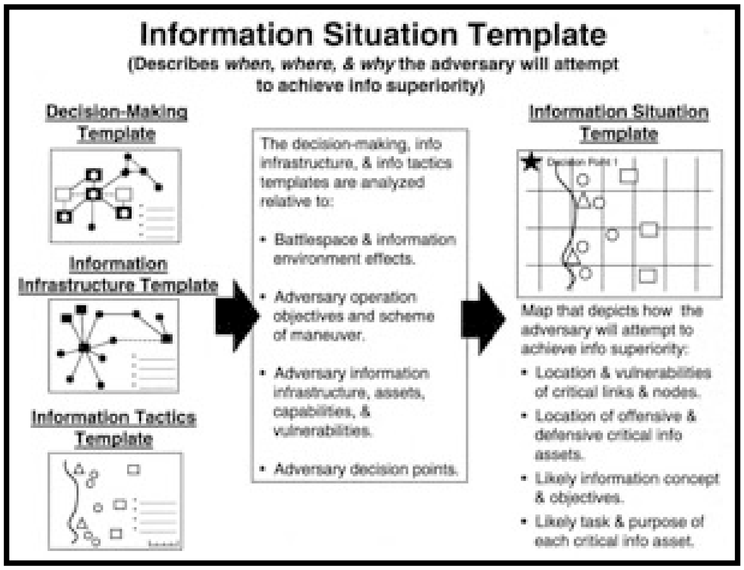
Information Situation Template
(Describes when, where, & why the adversary will attempt to achieve info superiority)
Decision-Making Template
Information Infrastructure Template
Information Tactics Template
The decision-making, info infrastructure, & info tactics templates are analyzed relative to:
• Battlespace & information environment effects.
• Adversary operation objectives and scheme of maneuver.
• Adversary information infrastructure, assets, capabilities, & vulnerabilities.
• Adversary decision points.
Information Situation Template
Decision Point 1
Map that depicts how the adversary will attempt to achieve info superiority:
• Location & vulnerabilities of critical links & nodes.
• Location of offensive & defensive critical info assets.
• Likely information concept & objectives.
• Likely task & purpose of each critical info asset.

Figure 4. Constructing an Information Situation Template.

Conclusion.

Templating the information threat allows us to evaluate the adversary's information system by identifying those assets and functions the adversary commander requires for decision-making and determining how the adversary will attack our information system while defending its own. In turn, this allows us to identify adversary vulnerabilities that friendly forces can exploit with IO and adversary offensive information capabilities that must be defended against.

Templates are powerful tools. When properly developed and used, templates can provide insight into how the adversary will employ its information assets and, perhaps more importantly, the location (in time, space, and purpose) of the adversary's critical vulnerabilities. Templating the information threat allows us to see our own information systems in relation to the adversary and terrain. In turn, this allows friendly forces to develop adversary courses of action (statement and sketch) so that we can visualize the future fight.

End Notes

[1] For the purpose of this article, the term "information IPB" is used rather than "IO IPB". This decision is based on the belief that the purpose of an information-based IPB is not to analyze information operations itself, but rather to analyze the information environment in which the command will operate.

[2] IO planners and analysts should be careful not to describe or portray adversary actions as a mirror image of U.S. doctrine. It is highly unlikely that an adversary's operations in the information environment will equate to our own. For this reason, the authors will not use the term IO in connection with describing adversary forces or operations.

[3] According to Joint Pub 1-02, an information system is the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. To focus on, and predict, adversary decision-making, it is useful to think of an information system as leaders/decision-makers, information infrastructures, and decision-making processes required to support military decision-making.

[4] The templating charts are based on LIWA Information Operations (IO) Handbook (Draft), October 1998, page 5-10, (US Army Land Information Activity, Fort Belvoir, VA).

Lieutenant Colonel David C. Grohoski is currently the Chief of the U.S. Army Land Information Warfare Activity (LIWA) Field Support Division. A career infantry officer, his previous assignments include Battalion Senior Observer/Controller at the Joint Readiness Training Center (JRTC), Exchange Officer in the British Army, Executive Officer of The Old Guard, as well as assignments in Light Infantry and Airborne Ranger Units. He is a Distinguished Military Graduate of Michigan State University and received a Masters Degree from the University of Oklahoma.

Major Marc J. Romanych (U.S. Army Retired) is a former Air Defense Artillery Officer. He works for JB Management Inc., contracted to the U.S. Army Land Information Warfare Activity (LIWA). Since 1998, he has deployed with LIWA information operations field support teams to Bosnia and on numerous Joint and Army warfighter exercises. He holds degrees in Chemistry, Geology, History, and International Relations. Readers may contact him via e-mail at mjroman @ vulcan.belvoir.army.mil or mjromanych@cs.com.